Sharing Beliefs about Actions: A Parallel Composition Operator for Epistemic Programs

Penelope Economou
Oxford University
Computing Laboratory
Oxford, OX1 3QD, UK
penelope.economou@comlab.ox.ac.uk
Themes

- A new operator on epistemic programs expressing the action of sharing a belief about the current action inside a subgroup.
- An equational calculus for this operator.
- Examples of its usage.
State Models

Given a set $\Phi_0$ of atomic propositions and a set of agents $\mathcal{A}$, an **(epistemic) state model** is a Kripke model

$$\mathcal{S} = (S, \rightarrow^A S, \parallel \cdot \parallel_s)_{A \in \mathcal{A}}$$

consisting of

1. a set $S$ of "states"
2. a family of binary accessibility relations $\rightarrow^A S \subseteq S \times S$, one for each agent $A \in \mathcal{A}$
3. and a **valuation** $\parallel \cdot \parallel_s : \Phi_0 \rightarrow \mathcal{P}(S)$, assigning to each fact $p \in \Phi_0$ a set $\parallel p \parallel_s$ of states
**Epistemic Propositions**

Let $S\text{Mod}$ be the collection of all state models. An **epistemic proposition** is an operation $\varphi$ defined on $S\text{Mod}$ such that for all $S \in S\text{Mod}$, $\varphi_S \subseteq S$.

If $s \in \varphi_S$, we say that state $s \in S$ **satisfies proposition** $\varphi$, or that $\varphi$ is **true** at state $s$ in model $S$. 
An (epistemic) action model is a Kripke model

\[ \Sigma = (\Sigma, \xrightarrow{A}, \text{pre})_{A \in A} \]

where
1. \( \Sigma \) is a set of simple actions,
2. \( \xrightarrow{A} \) is an \( A \)-indexed family of relations on \( \Sigma \), and
3. \( \text{pre} : \Sigma \rightarrow \mathcal{P}(\Phi_0) \).

An epistemic program is defined as a pair \( \pi = (\Sigma, \Gamma) \) consisting of an action model \( \Sigma \) and a set \( \Gamma \subseteq \Sigma \) of designated simple actions, which we often denote by \( |\pi| \).
Repackaging the Arrows

Epistemic programs can alternatively be presented by having maps:

$$
\pi_A : \Sigma \rightarrow \mathcal{P}(\Sigma), \quad \sigma \mapsto \sigma_A \subseteq \Sigma,
$$

for every agent \( A \in \mathcal{A} \), instead of the arrows.

If we are given the arrows \( A \rightarrow \), we can define the appearance \( a \):

$$
\sigma_A = \{ \sigma' : \sigma \rightarrow \sigma' \} \text{ to each agent } A.
$$

\(^a\)The appearance sets express the agents beliefs about the very action that is taking place. Thus, \( \sigma' \in \sigma_A \) represents the actions that an agent considers as ‘alternatives’ of the ‘real’ action.
To give an abstract specification of an *epistemic action* in a (given) epistemic model it is enough to define its:

1. preconditions $\text{pre} (\sigma)$

2. appearance $\sigma_A = \{ \sigma' : \sigma \xrightarrow{A} \sigma \}$ to each agent $A$.

An epistemic program is specified by defining all the actions $\sigma \in \Sigma$ in the model, and in addition giving the set of designated actions $|\pi|$. 

---

Sharing Beliefs about Actions: A Parallel Composition Operator for Epistemic Programs – p. 7/2
Motivation: An Epistemic Scenario

**Scenario 1: Pick a card.** A and B enter a large room containing a remote-control mechanical coin flipper. One presses the button and the coin spins through the air and then lands in a small box on a table. A card is shown to A, in the presence of B, which either says heads (H), tails (T), or is blank. In the first two cases the card describes truly the state of the coin in the box, and in the last case the intention is that no information is given.
A Representation of the Epistemic Program

\[ A, B \]

\[ \text{H} \]

\[ \text{T} \]

\[ B \]

\[ A, B \]
Our goal

- Propose a theoretical understanding of the above representation.
Our goal

- Propose a theoretical understanding of the above representation.
- ‘How are we going to model this epistemic action?’
Our goal

- Propose a theoretical understanding of the above representation.
- ‘How are we going to model this epistemic action?’
- Introduce a new operation that models the beliefs of the agents about the current action taking place and the justifiable changes affecting these beliefs.
Our goal

- Propose a theoretical understanding of the above representation.
- ‘How are we going to model this epistemic action?’
- Introduce a new operation that models the beliefs of the agents about the current action taking place and the justifiable changes affecting these beliefs.
- Introduce and discuss our logic after which we revisit the example scenario and show how it can be modeled.
Our goal

- Propose a theoretical understanding of the above representation.
- ‘How are we going to model this epistemic action?'
- Introduce a new operation that models the beliefs of the agents about the current action taking place and the justifiable changes affecting these beliefs.
- Introduce and discuss our logic after which we revisit the example scenario and show how it can be modeled.
- Demonstrate the usage of our new operation by examining a more complicated epistemic scenario.
Sharing Beliefs: While $\pi$, $B$ announces $\pi'$ to $C$. Given a group of agents $B, C \subseteq A = \{A, B \ldots \}$, and epistemic programs $\pi$, and $\pi'$, we introduce a new operation $\pi !^C_B \pi'$, to be read as: \textit{while} $\pi$, $B$ announces $\pi'$ to $C$.

Remarks:

- It represents a kind of \textit{parallel composition}: program $\pi$ is happening in parallel with a \textit{sincere, private}, (but \textit{not necessarily truthful}) announcement (from $B$ to $C$) that the program $\pi'$ is happening.
A New Operation on Epistemic Programs

Sharing Beliefs: While $\pi$, $B$ announces $\pi'$ to $C$. Given a group of agents $B, C \subseteq A = \{A, B \ldots\}$, and epistemic programs $\pi$, and $\pi'$, we introduce a new operation $\pi !^B_C \pi'$, to be read as: while $\pi$, $B$ announces $\pi'$ to $C$.

Remarks:

- It represents a kind of parallel composition: program $\pi$ is happening in parallel with a sincere, private, (but not necessarily truthful) announcement (from $B$ to $C$) that the program $\pi'$ is happening.

- While $\pi$ is happening (all members of) $B$ believe that $\pi'$ is happening instead, and moreover, they communicate this belief to (all members) of $C$ by sending (them) a message over a fully private, secure and reliable channel.
A New Operation on Epistemic Programs

Sharing Beliefs: While $\pi$, $B$ announces $\pi'$ to $C$. Given a group of agents $B, C \subseteq A = \{A, B \ldots\}$, and epistemic programs $\pi$, and $\pi'$, we introduce a new operation $\pi!^B_C \pi'$, to be read as: while $\pi$, $B$ announces $\pi'$ to $C$.

Remarks:

- After the group announcement by $B$ it becomes *common knowledge* among (the agents of) $B \cup C$ that $B$ believes $\pi'$. 
Sharing Beliefs: While $\pi, B$ announces $\pi'$ to $C$. Given a group of agents $B, C \subseteq A = \{A, B \ldots\}$, and epistemic programs $\pi$, and $\pi'$, we introduce a new operation $\pi !^B_C \pi'$, to be read as: while $\pi, B$ announces $\pi'$ to $C$.

Remarks:

- After the group announcement by $B$ it becomes *common knowledge* among (the agents of) $B \cup C$ that $B$ believes $\pi'$.

- However, the beliefs of the agents in $C$ are not changed by $B$'s announcement, i.e. they don't assume that $B$'s beliefs are truthful.
Abstract Definition of the New Operation

We can characterize our new operation by specifying the preconditions and appearances:

\[
\begin{align*}
| \pi \downarrow^B_C \pi' | & = \{ \sigma \downarrow^B_C \pi' : \sigma \in |\pi| \} \\
\text{pre}(\sigma \downarrow^B_C \pi') & =: \text{pre}(\sigma) \\
(\sigma \downarrow^B_C \pi')_B & =: \{ \sigma' \downarrow^B_C \pi' : \sigma' \in |\pi'| \}, \text{ for all } B \in B \\
(\sigma \downarrow^B_C \pi')_C & =: \{ \lambda \downarrow^B_C \pi' : \lambda \in \sigma_C \}, \text{ for all } C \in C \setminus B \\
(\sigma \downarrow^B_C \pi')_D & =: \sigma_D, \text{ for all } D \notin \{B, C\}
\end{align*}
\]
**Definition.** Given a set of *atomic propositions* $\Phi_0$ whose elements are usually denoted by $p$, $q$, $r$ and so on, the top and bottom element $\top$, and $\bot$, and a set of agents $B, C \subseteq A = \{A, B \ldots \}$, the formal definition of the well-formed *basic programs* of the *language* of DEC is given by

\[
\pi ::= ?p \mid \pi + \pi' \mid \pi \cdot \pi' \mid \pi !^B_C \pi'
\]

where $p$ ranges over $\Phi_0$. 
Reasons for Choosing our Basic Operations

They are the natural operations on epistemic programs and most others can be defined in terms of them. For example,

- \( \text{skip} \overset{\text{def}}{=} ?\top \), and \( \text{crash} \overset{\text{def}}{=} ?\bot \)

As far as \( \pi \up_B^C \pi' \) and according to the choice of \( \pi, \pi', B, \) and \( C \), we get:

- \( \pi \up_A^B \pi' \overset{\text{def}}{=} \pi \up_B \pi' \), obtained by taking \( C = A \). We call this: *public announcement of a program by subgroups.*
Reasons for Choosing our Basic Operations

- \( \pi !^B_{\pi'} \overset{\text{def}}{=} \pi |^B \pi' \), obtained by taking \( B = C \). We read this: while \( \pi, B \) thinks \( \pi' \).

The following are all special cases of the above:

- \( B_{\pi} \overset{\text{def}}{=} \text{skip} |^B \pi \). We call this: gratuitous (i.e. mistaken) group updating with a program.

- \( L^B_{\pi} \overset{\text{def}}{=} \pi |^B \pi \). We call this: group learning of a program.

Finally, we have

- \( ?p !^B_{\pi} p \overset{\text{def}}{=} p!_B \), where \( p!_B \) is the totally private, truthful announcement of an atomic proposition \( p \) to only to a subgroup \( B \subseteq A \).
Axioms of DEC

We propose some natural axioms for each of our operators:

- $(+)$ is associative, commutative, idempotent, and has $crash$ as a neutral element.

- $(\cdot)$ is associative as well as right and left distributive over $(+)$.

- A natural axiom for $(\cdot)$ is: $skip \cdot x = x \cdot skip = x$. 
Axioms of DEC

We continue with some natural axioms for (?)

\[ ?p \cdot ?p = ?p \] (t1)
\[ ?p \cdot x = x \cdot ?p \] (t2)
\[ ?p = ?p !B skip \] (t3)
\[ ?p \cdot (?p !B_C x) = ?p !B_C x \] (t4)
Axioms of DEC

Finally, here are some natural axioms for $(!^B_C)$

\[
(x + y)!^B_C z = x!^B_C z + y!^B_C z \quad (a1)
\]

\[
(x!^B_C y) \cdot (z!^B_C w) = ((x!^B_C y) \cdot z)!^B_C ((y!^B_C y) \cdot w) \quad (a2)
\]

\[
(x!^B_C y)!^B_C (z!^B_C w) = x!^B_C z \quad (a3)
\]

\[
skip!^B_C skip = skip \quad (a4)
\]
The total action describing the epistemic scenario **Pick a Card** is:

\[ \pi = \sigma + \rho + \mu \]

where

\[ \sigma = (\mathcal{L}^A?H)!^B(\mathcal{L}^A?H + \mathcal{L}^A?T + \text{skip}) \]

\[ \rho = (\mathcal{L}^A?T)!^B(\mathcal{L}^A?H + \mathcal{L}^A?T + \text{skip}) \]

\[ \mu = \text{skip}!^B(\mathcal{L}^A?H + \mathcal{L}^A?T + \text{skip}) \]
The Epistemic Scenario Revisited

As $\pi$ is non-deterministic, it can be resolved in any way $\sigma$, $\rho$, or $\mu$ are resolved:

$$|\pi| = \{\sigma\} \cup \{\rho\} \cup \{\mu\}.$$  

Simple actions $\sigma$, $\rho$, and $\mu$ can happen if the card is showing heads, tails or nothing, respectively:

$$\text{pre}(\sigma) = H, \text{pre}(\rho) = T, \text{and} \ \text{pre}(\mu) = T.$$  

And finally:

- $(\sigma)_A = \sigma$, $(\rho)_A = \rho$ and $(\mu)_A = \mu$
- $(\sigma)_B = (\rho)_B = (\mu)_B = \{\sigma\} \cup \{\rho\} \cup \{\mu\}.$
Man-in-the-middle (MITM) Attack

**Problem:** Epistemic operators already existing in the literature (Baltag, Gerbrandy, and van Ditmarsh) are too simple or not enough to handle the MITH scenario.

**Solution:** We claim that the epistemic program describing the variant of the MITM attack (to be described shortly) can be expressed in (the language of) DEC using the parallel composition operator introduced earlier.
The epistemic program describing a variant of the (MITM) attack has the following representation:

```
\[
\begin{align*}
C & \xrightarrow{\sigma} \quad B & \xrightarrow{\rho} \\
A, B, C & \xrightarrow{\sigma'} & A, B, C
\end{align*}
\]
```
The total action where the secret \((p, \text{ or } \neg p)\) is intercepted, modified and resent to \(B\) is \(\sigma + \rho\). We claim that:

\[
\sigma = \sigma'' \mid^C (\sigma'' + \rho'') \quad \text{and} \quad \rho = \rho'' \mid^C (\sigma'' + \rho''),
\]

where

\[
\sigma'' = (\neg p) \cdot (A(p!_{A,B}) \cdot B((\neg p)!_{A,B}))!^C (p!_{A,B} + (\neg p)!_{A,B} + \text{skip})
\]

\[
\rho'' = (p) \cdot (A((\neg p)!_{A,B}) \cdot B(p!_{A,B}))!^C (p!_{A,B} + (\neg p)!_{A,B} + \text{skip})
\]
We also claim that

\[ \sigma' = (p!_{A,B})^C (p!_{A,B} + (\neg p)!_{A,B} + \text{skip}) , \]

\[ \rho' = ((\neg p)!_{A,B})^C (p!_{A,B} + (\neg p)!_{A,B} + \text{skip}) , \]

and

\[ \gamma = \text{skip}^C (p!_{A,B} + (\neg p)!_{A,B} + \text{skip}) . \]
A Representation of the Epistemic Program

According to the action model above, we should have:

- $\sigma_C = \rho_C = \{\sigma\} \cup \{\rho\}$
- $\sigma_A = \rho_B = \sigma', \rho_A = \sigma_B = \rho'$, $\gamma_A = \gamma_B = \gamma$,
- $\sigma'_C = \rho'_C = \gamma = \{\sigma'\} \cup \{\rho'\} \cup \{\gamma\}$
- $\sigma'_A = \sigma'_B = \sigma'$, $\rho'_A = \rho'_B = \rho'$. 
Conclusions

We introduced a new operation with epistemic programs i.e. $\pi !^{B_C} \pi'$ expressing the action of sharing a belief about the current action inside a subgroup.
Conclusions

- We introduced a new operation with epistemic programs i.e. \( \pi \uparrow_B^C \pi' \) expressing the action of sharing a belief about the current action inside a subgroup.
- We showed that many useful programs can be defined by \( \pi \uparrow_B^C \pi' \).
Conclusions

- We introduced a new operation with epistemic programs i.e. $\pi \downarrow^B C \pi'$ expressing the action of sharing a belief about the current action inside a subgroup.
- We showed that many useful programs can be defined by $\pi \downarrow^B C \pi'$.
- We proposed an equational calculus for this operation.
Conclusions

- We introduced a new operation with epistemic programs i.e. $\pi \mid^B_C \pi'$ expressing the action of sharing a belief about the current action inside a subgroup.
- We showed that many useful programs can be defined by $\pi \mid^B_C \pi'$.
- We proposed an equational calculus for this operation.
- We gave two examples of its usage, of which is a variant of the well-known (MITM) attack.
Future Work

- Prove completeness of the equational calculus.

- Explore the expressive power of the calculus. For example, a natural question would be: "Which actions and action operations can be defined by terms in the equational calculi?"

- Demonstrate the use of the calculus in the analysis of distributed systems.

- Extend the range of $p$ (in our proposed syntax) from atomic to epistemic propositions and try and develop a complete calculus for epistemic programs and epistemic propositions.
Future Work

- Prove completeness of the equational calculus.
- Explore the expressive power of the calculus. For example, a natural question would be: "Which actions and action operations can be defined by terms in the equational calculi?"
Future Work

- Prove completeness of the equational calculus.
- Explore the expressive power of the calculus. For example, a natural question would be: ”Which actions and action operations can be defined by terms in the equational calculi”?
- Demonstrate the use of the calculus in the analysis of distributed systems.
Future Work

- Prove completeness of the equational calculus.
- Explore the expressive power of the calculus. For example, a natural question would be: ”Which actions and action operations can be defined by terms in the equational calculi”?
- Demonstrate the use of the calculus in the analysis of distributed systems.
- Extend the range of $p$ (in our proposed syntax) from atomic to epistemic propositions and try and develop a complete calculus for epistemic programs and epistemic propositions.